ISE

INFORMATION SHARING ENVIRONMENT
ANNUAL REPORT TO THE CONGRESS

NATIONAL SECURITY THROUGH RESPONSIBLE INFORMATION SHARING

Prepared by the
Program Manager, Information Sharing Environment

30 June 2014

sharing
information
National
Intelligence
implementation
Group
centers
Interagency
DHS
Departments
critical
collaboration
ensure
Initiative
classified
Strategy
report
common
system
develop
use
public
integration
existing
Secret
Executive
needs
including
providing
Police
data

ISE

fusion
mission
securi
across
Department
Agency
NIEM
Services
Performance
Maritime
infrastructure
interoperability
policies
guidance
effort
Office
analysts
privacy
areas
government
state
systems
terrorism
Criminal
law
work
best
key

CONTENTS

INTRODUCTION TO THIS REPORT

This report is submitted by the Program Manager for the Information Sharing Environment (PM-ISE) on behalf of the President, as required by Section 1016 (h) (2) of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended.

Accompanying, but distinct from this report, are substantial performance data and links to best practices, lessons learned, frameworks, and initiatives that are increasingly being packaged as reusable tools and accessed broadly via the Information Sharing Environment's Web site: www.ise.gov. In past years this material was directly integrated into this report. Accomplishments, opportunities, and the way forward described in this report are based on this qualitative and quantitative performance data, as reported to the Office of the Program Manager, Information Sharing Environment by various agencies; on performance trends year-by-year; and on the evolution of priority threats as they have been identified, and changes in our operating environment. Readers of this report are encouraged to dig deeper into specific topics of interest via our Web site.

In December 2012, the President released the National Strategy for Information Sharing and Safeguarding (2012 Strategy). Subsequently, the White House and the PM-ISE released the 2012 Strategy's Strategic Implementation Plan. The 2012 Strategy and its implementation plan defined the general vision and framework for responsible information sharing across the national security and public safety environments, and provide the specific efforts needed to continue maturing the Information Sharing Environment. Both documents build on and integrate the tools and initiatives reflected in our nation's tremendous investment in terrorism-related information sharing. Positioning these tools and initiatives for reuse and further integration into the overall national security framework shapes the discussion in this report.

VISIT WWW.ISE.GOV FOR MORE DETAILS

FOREWORD FROM THE PROGRAM MANAGER

Our national security and public safety rely upon responsible information sharing between federal, state, local, and tribal agencies, private sector entities, and international partners. Collaboration between all of these stakeholders is essential in order to create an enduring Information Sharing Environment (ISE) in which information is managed as a national asset, sharing and safeguarding are effectively integrated, and information sharing informs the decisions made to ensure the security of the nation and the safety of the American people. In order to progress we must strengthen and mature our management processes to better align disparate and independent efforts, within a strong foundation of protection for privacy, civil rights, and civil liberties.

The national investment in terrorism-related information sharing has led to the development of policies, systems, and standards that enable the nation to address related priority threats, including physical and cyber threats to our critical infrastructure, transnational organized crime, human trafficking, drug trafficking, and illicit financial networks. Leveraging the processes and tools we have already developed, and integrating information on a wider range of threats will strengthen the ISE, accelerate the delivery of new capabilities, and improve decision making and program effectiveness.

The ISE framework was created in response to the demands of our stakeholders for ways to enhance information sharing at all levels of government. We see this most clearly with state and local agencies and programs like the National Network of Fusion Centers and other field-based information-sharing entities that recognize the critical need to share information in disciplined and efficient ways. These agencies and programs are seeking ways to meet their responsible information sharing challenges under their own authorities. They represent communities that have common interests in establishing information sharing environments to overcome cultural, technical, and legal impediments to information sharing. These communities complement top-down efforts to realize the vision of a decentralized, distributed, and coordinated ISE, as defined by the attributes in the IRTPA of 2004, as amended.

My primary duties as Program Manager are to be the premier advocate for responsible information sharing; to promote secure and trusted, whole-of-government collaboration; and to accelerate mission impact to counter terrorism and other priority threats. My office supports these communities through transparency, participation, and collaboration with federal, state, local, and tribal agencies, private sector entities, international partners, industry associations, public-private collaborations, academic and research entities, and standards organizations.

Communities of Interest form around shared mission objectives to address significant national problems and challenges. The Communities of Interest that we now serve are focused on the following mission areas: the sharing and use of public safety information via statewide and regional ISEs; improving watchlisting, screening, and encounters; cybersecurity information sharing; advancing information sharing of air and maritime domain awareness; and improving first responder incident information sharing and response. An emerging area of focus is leveraging the tools and initiatives of the ISE to counter transnational organized crime. In addition, we are seeing agencies self-organize Communities of Interest in the nexus between public health and public safety.

We provide support to these Communities of Interest in two ways. First, we generate an increasingly shared vision that reduces fragmentation, overlap, duplication, and information gaps by integrating existing initiatives and advancing information interoperability. Second, we help them increase their effectiveness by developing ISE tools and initiatives that are easier to use, and by promoting collaboration between subject matter experts.

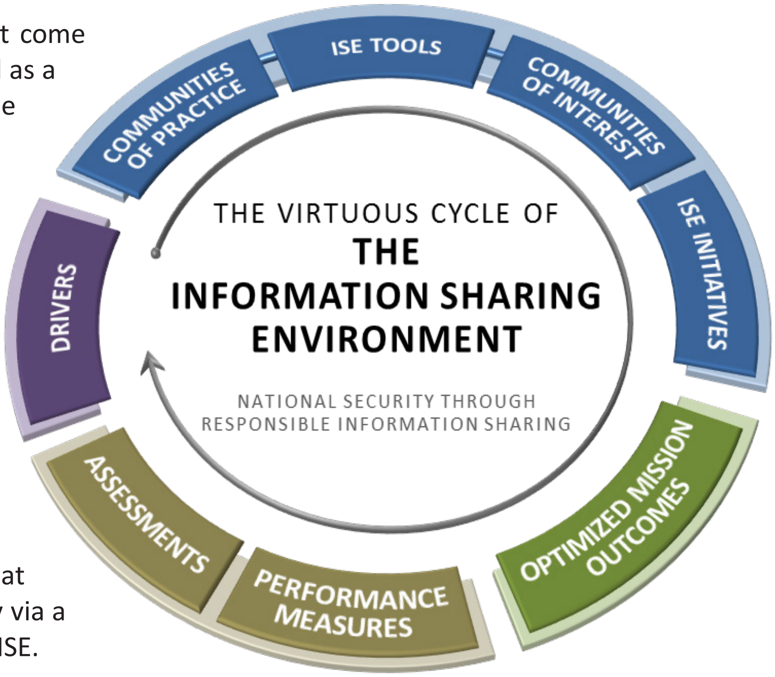
These tools and initiatives are increasingly anchored in Communities of Practice, which are coalitions of people with interest and expertise in various aspects of information sharing. In line with our commitment to open government, we are promoting these communities through open forums such as those associated with standards organizations, industry associations, and public-private collaborations. These open forums are actively honing ISE tools and initiatives for use on mission objectives; their use of these tools and initiatives has been proven to reduce risk and cost, drive innovation, accelerate mission impact and agility, and consequently improve responsible information sharing. As Communities of Interest pursue initiatives that continue to leverage and extend ISE tools and initiatives anchored in Communities of Practice, agencies and private sector entities will gain an ever-more-accessible pathway toward realizing these benefits.

Kshemendra N. Paul
Program Manager, Information Sharing Environment

ACCELERATING MISSION IMPACT

To further accelerate mission impact and homeland security information sharing, agencies are identifying and aligning the Communities of Interest that are responsible for addressing specific priority threats, including terrorism and homeland security information sharing. This process is the next step in our collective efforts, beyond the publication of the 2012 Strategy's Strategic Implementation Plan. Capstone governance for this process is provided by the White House's Information Sharing and Access Inter-Agency Policy Committee, co-chaired by the National Security Council staff's Senior Director for Information Sharing and Access and the Program Manager for the ISE. This committee works with departments and agencies to identify and resolve information sharing issues in accord with Section 1016 (g) of the IRTPA.

Solutions for these Communities of Interest come from leveraging ISE tools and initiatives, and as a result advance the priority objectives of the 2012 Strategy. We have matured our management frameworks to allow us to orient first on the mission, and second on enabling tools and initiatives. Through this dual focus PM-ISE has been able to demonstrate progress toward the priority objectives in the 2012 Strategy.



When this cycle of responsible information sharing is self-sustaining, we will be materially closer to our vision of secure and trusted collaboration that enhances national security and public safety via a decentralized, distributed, and coordinated ISE.

INFORMATION SHARING ENVIRONMENT

The ISE "provides and facilitates the means for sharing terrorism information among all appropriate federal, state, local, and tribal entities, and the private sector through the use of policy guidelines and technologies."[1]

ISE MISSION FOCUS

Statewide & Regional ISEs

Facilitate the sharing of terrorism and homeland security information among all appropriate federal, state, local, tribal, and territorial entities, and the private sector

Watchlisting, Screening & Encounters

Supports the ability of agencies to identify known or suspected terrorists trying to obtain visas, enter the country, board aircraft, or engage in terrorist-related activity

Cybersecurity Information Sharing

Applying lessons learned to broadly improve the sharing of cyber threat and incident information as a means to improve cybersecurity

Domain Awareness

The effective understanding of information associated with maritime and air domains that could impact the security, safety, economy, or environment of the United States

Incident Management

The broad spectrum of activities and organizations that provide effective and efficient operations, coordination, and support . . . to plan for, respond to, and recover from an incident

[1] Section 1016 (b) (2), IRTPA, as amended.

THE 2013 BOSTON MARATHON BOMBING – APPLYING LESSONS LEARNED

In April 2013, the nation witnessed a terrorist strike on Boston's Boylston Street: since then, we have all seen the resilience and strength of the Boston community.

> "[W]e should take time to look at what lessons have been learned since the (Boston Marathon bombings) and how we can improve our defenses against attacks in the future."
>
> — Chairman Michael McCaul, House Committee on Homeland Security, April 8, 2014

In April 2014, the Inspectors General of the Intelligence Community, the Central Intelligence Agency (CIA), the Department of Justice (DOJ), and the Department of Homeland Security (DHS) issued a report examining the U.S. government's handling and sharing of information prior to the Boston Marathon bombings.[2]

Based on all the information gathered during a coordinated review, the Inspectors General concluded that the Federal Bureau of Investigation (FBI), the CIA, DHS, and the National Counterterrorism Center (NCTC) had generally shared information and followed procedures appropriately. However, they did identify some areas where broader information sharing between agencies may have been required, and where broader information sharing in the future should be considered: for example, greater sharing of threat information with state and local partners.[3]

With respect to the FBI's pre-bombing investigation, the Inspectors General concluded that the FBI made investigative judgments based on information known at the time and that were within the legal framework governing its ability to gather intelligence and conduct investigations, in this case, of U.S. Persons.

Each participating Office of the Inspector General (OIG) reached conclusions about the actions taken or not taken by its component agencies. Among the most significant conclusions described in the public summary were the following:[4]

- The DOJ OIG concluded that, given the limited information available to the Boston Joint Terrorism Task Force (JTTF) in March 2011 concerning Tamerlan Tsarnaev, one of the two alleged bombers, the FBI's decision to open the investigation at the assessment level was within its investigative discretion as an application of the "least intrusive method" principle set forth in the Attorney General Guidelines for Domestic FBI Operations and the FBI's Domestic Investigations and Operations Guide. They found that additional investigative steps would have

[2] Unclassified Summary of Information Handling and Sharing Prior to the April 15, 2013 Boston Marathon Bombings, Prepared by the Inspectors General of the: Intelligence Community, Central Intelligence Agency, Department of Justice, and the Department of Homeland Security, 10 April 2014.

[3] Ibid, p. 21.

[4] Ibid.

resulted in a more thorough assessment, but concluded that it is impossible to know whether these additional steps would have yielded relevant information.

- The DHS OIG examined whether Customs and Border Protection (CBP) had vetted Tsarnaev's outbound travel to Russia according to policies and procedures, and determined that it had done so.
- The DHS OIG determined that CBP properly admitted Tsarnaev into the United States in July 2012 after taking his picture, collecting his fingerprints, and confirming his identity and his status as a lawful permanent resident.
- The DHS OIG examined the adjudication of Tamerlan Tsarnaev's 2012 application for naturalization by the U.S. Citizenship and Immigration Services (USCIS) and concluded that, with one exception, the USCIS conducted the naturalization processes in accordance with the requirements of the Immigration and Nationality Act, and USCIS policies and procedures. Further, they determined that had USCIS conducted the omitted check, it would not have found additional information related to Tsarnaev's 2012 application for naturalization.

The **Boston Regional Intelligence Center (BRIC)** performs and coordinates regional homeland security protection and response missions through investigative and analytical activities. These activities are vital to the region's ability to identify and interdict terrorist operations. The BRIC is structured and centered on liaison-driven, collaborative information sharing between metropolitan Boston communities, private sector stakeholders, universities, and state and federal partners.

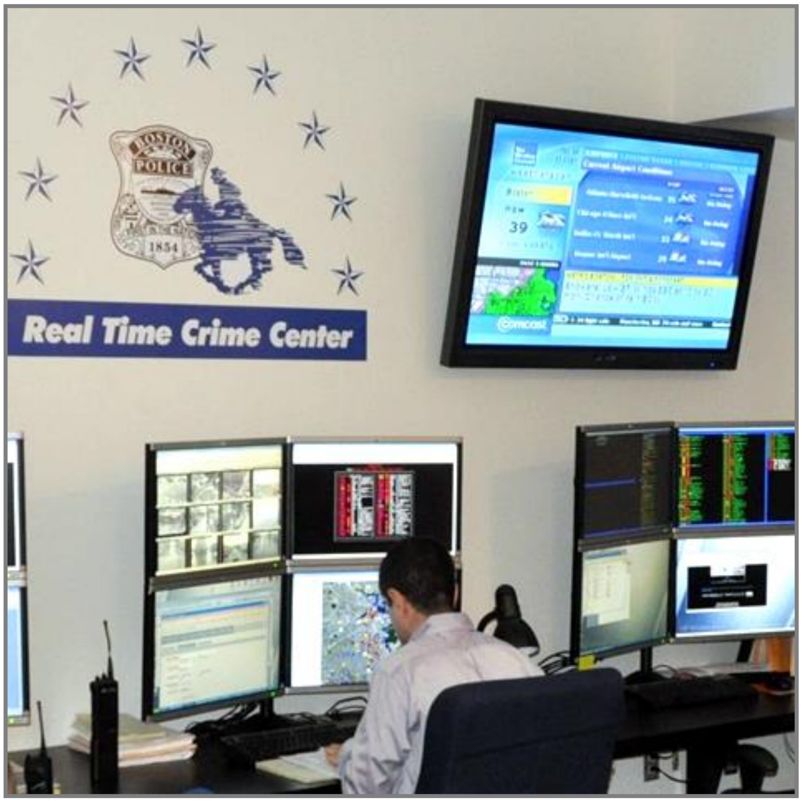


Photo Courtesy of the Boston Police Department

The Inspectors Generals' report recommends that the FBI and DHS clarify JTTF alert procedures and that the FBI consider sharing threat information with state and local partners more proactively and uniformly by establishing a procedure for notifying state and local representatives on JTTFs when it conducts a counterterrorism assessment of a subject having a nexus to a representative's area of responsibility. In response to the report's recommendations, DHS has updated guidance to officers at the JTTF to improve collaboration with the FBI.[5]

In the aftermath of the Boston attack, collaboration and information sharing between federal, state, and local stakeholders was highly effective.[6] Across the board, informed commentary lauded the teamwork. Notable was the FBI's investigative leadership; the role of local and state police in the apprehension of suspects; and the effectiveness of the National Network of Fusion Centers, the Homeland Security Information Network, and other ISE frameworks and initiatives in providing authoritative and real-time situational awareness and investigatory support across the country.

Since the Boston attack, DHS, the FBI, NCTC, the National Network of Fusion Centers, and other state and local agencies have expanded information sharing about potential threats. Additionally, DHS continues to work closely with federal partners to screen and vet domestic and international travelers, visa applicants, and other persons of interest to identify potential threats.[7]

Lessons learned from the Boston Marathon bombing align with multiple ISE mission areas, notably watchlisting, screening, and encounters; statewide and regional ISEs; and incident management. The report's findings and recommendations provide us with opportunities to improve responsible information sharing within relevant Communities of Interest, particularly in the proactive, bi-directional, and uniform sharing of intelligence and information with state and local law enforcement.

[5] Ibid, p. 25.

[6] Leonard, Cole, Howitt and Heymann. *Why* Was Boston Strong?: Lessons from the Boston Marathon Bombing (Cambridge: Harvard Kennedy School Program on Crisis Leadership, 2014), p. i.

[7] Unclassified Summary of Information Handling and Sharing Prior to the April 15, 2013 Boston Marathon Bombings, Prepared by the Inspectors General of the: Intelligence Community, Central Intelligence Agency, Department of Justice, and the Department of Homeland Security, 10 April 2014, DHS Management Comments.

PROGRESS TOWARD STRATEGIC GOALS

The President's 2012 Strategy laid out five goals, which are in effect critical success factors for creating an ISE for the nation. The Office of the PM-ISE is focused on implementing these goals. What follows in this report describes the challenges, accomplishments, and opportunities for making progress toward each of the goals in the 2012 Strategy.

DRIVE COLLECTIVE ACTION THROUGH COLLABORATION AND ACCOUNTABILITY

> As the components of the ISE are deployed across Communities of Interest in the execution of their respective missions, the process of adoption has led to increased collaboration on issues of national as well as local significance, to the point where whole Communities of Interest are acting in concert. The result has been evident in matters such as the common baseline capabilities defined for fusion centers.

CHALLENGE

This report and previous annual reports highlight how terrorism-related information sharing has improved since September 11, 2001, both across federal agencies, and between federal, state, and local agencies. However, from the broader scope defined in the 2012 Strategy, several challenges remain. The Federal Government still lacks sufficient cross-agency intelligence and information sharing processes and procedures for assessing and sharing terrorism-related information with private sector partners, particularly with respect to cybersecurity threats.

Building on the past year's findings, there continues to be a shortfall in developing and implementing a standard, interagency governance process for information sharing agreements between and among agencies at all levels of government. The findings indicate that departments and agencies are proactive in developing bilateral information sharing agreements when those agreements are of immediate value to their own missions. However, they are not incentivized to make their information discoverable and retrievable by other agencies when there is no immediate perceived reciprocal value. This challenge is at both the federal agency level and between federal, state, and local agencies.

Department and agency progress toward implementing the 2012 Strategy is uneven. Some agencies, such as the Departments of State and Homeland Security, are embracing implementation, have the requisite internal organizational maturity, and are providing stewardship for specific priority objectives in the 2012 Strategy. The Intelligence Community is advancing its transformational and aligned Information Technology Enterprise. Within the Departments of Defense and Justice, the level of participation is program-specific.

Further challenges stem from the broad-based nature of the 2012 Strategy's priority objectives. As previously described, in recognition of the differences in department and agency prioritization, maturity, and operating environments, implementation of the 2012 Strategy is shifting from a direct focus on priority objectives toward using mission-oriented Communities of Interest as vehicles for bringing about progress. This approach will accelerate the implementation of priority objectives and promote a broad-based adoption of solutions for impacting missions. The table below exemplifies this shift by showing the alignment of two mission Communities of Interest with related priority objectives.

Statewide and Regional ISEs	Watchlisting, Screening, and Encounters
Identity, Credential and Access Management (ICAM) is key to sharing granular law enforcement information broadly, where value is derived first locally; then between states; and finally, sharing between federal, state, and local entities.	**Information Sharing Agreements** involve moving to multi-lateral agreements that are built using consistent guidelines, and can be automated and more easily audited.
Baseline Interoperability Requirements and Standards-based Acquisition is key to industry adoption and scale-up via the procurement and emergence of shared, cloud-based, broadband services.	**Data Tagging** requires agreement on shared, managed attributes that have meaning across information sharing partners, to support consistency and automation with Information Sharing Agreements.
Nationwide Suspicious Activity Reporting (SAR) Initiative and National Network of Fusion Centers represent the premier standardization of law enforcement encounter information, with the National Network as the key to sharing threat intelligence, and information across federal, state, and local entities.	**Access & Discovery and Data Aggregation Reference Architecture** provides critical support to discovering non-obvious relationships, improving end-to-end process performance, and reducing costs and mission impact from current fragmentation, duplication, overlap, and gaps.

ACCOMPLISHMENTS

Departments and agencies made improvements in collaboration and interoperability across several Communities of Interest, as illustrated by the following accomplishments:

- ***Re-use of existing tools and technologies*** is an area where we continue to see progress by state and local partners, who are increasingly taking ownership of the maturation of the National Network of Fusion Centers.
- DHS and DOJ consolidated suspicious activity reporting into a single reporting mechanism known as ***the "Nationwide Suspicious Activity Reporting Initiative Shared Data Repository."*** The Repository streamlines terrorism-related suspicious activity reporting, eliminates overlapping or duplicative services, and reduces the risk of not connecting relevant terrorism-related information.
- NCTC and DHS recently ***automated NCTC's screening support for Electronic System for Travel Authorization (ESTA) applicants***. This automated process enables NCTC to inform DHS if an applicant has a nexus to terrorism, information which is then fed directly into the National Targeting Center's ESTA hotlist. Since the NCTC process is now automated, DHS can potentially use the NCTC information to revoke previously approved ESTA applications.

- The FBI's Terrorist Screening Center successfully deployed ***the Terrorist Encounter Reporting Application***, which provides users with the ability to more effectively document watchlist encounter information.
- The FBI's Terrorist Screening Center and DHS ***streamlined the delivery of Encounter information to the National Network of Fusion Centers*** using the Homeland Security Information Network (HSIN).
- The FBI and DHS, in concert with the National Network of Fusion Centers, ***initiated efforts to improve threat information sharing*** between federal government agencies and private sector partners.
- The FBI's Terrorist Screening Center and the U.S. Customs and Border Protection (CBP) ***automated the exchange of watchlist encounter information*** between the Terrorist Screening Operations Center and CBP's National Targeting Center.
- DOJ issued a policy memorandum for the heads of DOJ law enforcement components regarding the ***mandatory use of deconfliction systems in the course of all current and future investigative activity***.

OPPORTUNITIES

- ***Continue improving standard interagency governance processes*** for information sharing and safeguarding agreements that provide common requirements, procedures, and templates for use by ISE partners across all levels of government and industry.
- ***Develop consistent processes and reusable, standardized message templates*** for both Requests for Information and Alerts, Warnings and Notifications, to eliminate inconsistencies in information sharing across the ISE.
- ***Develop a maritime architecture plan*** that supports the National Maritime Domain Awareness Plan and provides a secure collaborative information sharing environment.
- ***Leverage current ISE tools*** across all departments and agencies ***against threats to the homeland posed by transnational organized crime***.

IMPROVE INFORMATION DISCOVERY AND ACCESS THROUGH COMMON STANDARDS

The use of common standards improves the interoperability of information systems, including the ability to automate enforcement of policy. This results in more information and data being usefully and quickly available, within a policy and mission context. In turn, agencies and private sector entities have the opportunity to further strengthen trusted and secure collaboration in order to more quickly address emerging threats; to protect public safety; and to enhance national security.

CHALLENGE

The Federal Government lacks a standardized approach to control access to and discovery of sensitive information on computer networks; and to include common processes to assure compliance with legal, regulatory, and mission-area policies. Consequently, users cannot consistently obtain reliable, timely, and repeatable discovery of and access to terrorism-related and homeland security information. This includes both human-initiated and machine-speed sharing and data analytics.

STANDARDS COORDINATING COUNCIL
SEARCH
Institute for Intergovernmental Research
OASIS
OMG
OBJECT MANAGEMENT GROUP
IJIS Institute
CJIS
AFCEA
AFEI
NIST
Global Justice Information Sharing Initiative
OGC
Open Geospatial Consortium, Inc.
ACT-IAC
Advancing Government
NIEM

In addition, some departments and agencies maintain proprietary information systems that support the individual agency's needs, but present a barrier to sharing relevant information with other government agencies and external partners and stakeholders.

ACCOMPLISHMENTS

Departments, agencies, and other key ISE partners have made improvements through the following accomplishments:

- ***Strengthened maturity and adoption of common standards across the public sector via the work of the Standards Coordinating Council.***
- ***Supported an industry-led effort to develop a cross-cutting, integrated threat and risk information model*** and supporting information exchange functional standards.
- The National Information Exchange Model (NIEM) Program Management Office, the Open Geospatial Consortium, DHS, and the Office of the PM-ISE ***worked together to strengthen the integration of geospatial tags into the ISE's information interoperability framework and***

associated standards, enabling the integration and sharing of valuable location information with mission operators and analysts.

- DHS ***completed an initial draft Geospatial Interoperable Reference Architecture (GIRA)*** for interagency coordination in response to the need for solutions to effectively govern, manage, support, and achieve interoperability through geospatial system integration, acquisition, or development.
- The Office of the PM-ISE ***developed an organizational maturity model, architecture, and associated standards, and supports pilot efforts***, like DHS's Data Framework and Common Entity Index Prototype, to help reduce fragmentation, overlap, duplication, and gaps in sharing and aggregating agency data sets.
- The Data Aggregation Working Group, under the direction of DHS and NCTC, ***completed an initial draft of a Data Aggregation Reference Architecture (DARA) for interagency coordination*** in response to the need for a reference architecture to support a consistent approach to discovery and data correlation across disparate data sets.
- The Office of the PM-ISE ***increased support for adoption, integration, and use of the information interoperability frameworks and tools***, under the label of *Project Interoperability*, with Communities of Practice anchored outside the government under the Standards Coordinating Council.
- The Global Standards Council of the Global Advisory Committee to the Attorney General has ***published a number of justice domain web services standards for adoption throughout the justice system***.
- The Office of the Director of National Intelligence ***engaged in facilitating a better understanding of Critical Infrastructure and Key Resources sectors' information needs*** through workshops, threat briefings, and joint information sharing pilot efforts with the aviation and critical manufacturing sectors within the National Infrastructure Protection Plan framework.

OPPORTUNITIES

- ***Align enterprise data management and data tagging*** across the Federal Government to enable discovery and access.
- ***Continue to establish enterprise dataset inventories*** within agencies, using a data reference model from the Federal Enterprise Architecture.
- ***Prioritize implementation of identity, credential, and access management*** through shared, interoperable, standards-based services to enhance authorized access and strengthen prevention of unauthorized access.
- ***Drive government-wide adoption of best practices and lessons learned***, like those from the Intelligence Community's Information Technology Enterprise, which is expected to enable greater integration, information sharing, and information safeguarding through a common Intelligence Community information technology approach.
- ***Further develop approaches to leverage common standards for procurement*** by federal, state, and local agencies for requisite common mission capabilities, building on initial national scale successes in the law enforcement and homeland security space.

- ***Continue maturing and applying best practices to integrate standards-oriented Communities of Practice with mission-oriented Communities of Interest across the ISE*** as a means of advancing information sharing and safeguarding.
- ***Better align nascent DHS cybersecurity information sharing specifications*** with mature, open, and voluntary consensus standards like NIEM, via the Standards Coordinating Council.
- ***Continue to refine elements of the ISE through a collaborative process***, using the Standards Coordinating Council.

OPTIMIZE MISSION EFFECTIVENESS THROUGH SHARED SERVICES AND INTEROPERABILITY

> Through shared services, agencies and private sector entities across Communities of Interest interconnect existing information sharing initiatives to support secure, interoperable, and trusted collaboration across a recognized national security and public safety platform that will enhance success in all mission areas.

CHALLENGE

The public safety and national security information technology enterprises are fragmented, with varying degrees of overlap, duplication, and capability gaps. Rather than adding to the problem by building new systems, a better approach is to focus on connecting existing systems and mission area capabilities through better alignment of agency management policies and practices that support common standards for information discovery and access.

Identifying and establishing needed capabilities, common requirements, and security controls for data interoperability will enable effective data exchanges between services, and interoperability between systems.

ACCOMPLISHMENTS

Departments, agencies, and other key ISE partners have made improvements through the following accomplishments:

- DHS has led the effort to expand ***simplified sign-on and interoperability across some of the nation's largest sensitive but unclassified law enforcement networks***, including Regional Information Sharing Systems (RISS), the Law Enforcement Enterprise Portal, the Homeland Security Information Network (HSIN) and Intelink, to over half a million registered users. These efforts are in the process of graduating, under the impetus of participating federal, state, and local departments and agencies, to a broader and more inclusive focus on shared capabilities.
- ***Successfully bridged two of the three nationally-used, event deconfliction services***—*RISSafe™* and *Case Explorer*; work continues to integrate *SAFETNet* into the federation. Also related is recent DOJ policy mandating event, investigatory, and subject deconfliction across all of its law enforcement components, which is having positive effects on other federal, state, local, and tribal law enforcement agencies.
- ***State and local partners continued to integrate interoperability tools***, as seen in RISS integration with HSIN, to provide improved identity proofing services.
- Use of HSIN enabled the National Network of Fusion Centers to ***streamline reporting and collaboration*** for the maturation of Fusion Liaison Officer Programs.

- ***States continued work on maturing their domestic information sharing architectures*** based on best practices, and continue to build accessible public safety data sets to enable sharing information in support of law enforcement, homeland security, and emergency management systems.
- The Department of Defense and the Office of the PM-ISE ***sponsored the Combating Transnational Organized Crime data sharing pilot program*** to enable federal, state, local, tribal, and territorial law enforcement agencies to establish a Transnational Criminal Organization-Homeland Defense data sharing enterprise.
- The Office of the PM-ISE ***supported efforts*** by the National Network of Fusion Centers, High Intensity Drug Trafficking Area Centers, RISS Centers, the Drug Enforcement Administration, and other federal, state, and local agencies ***to apply the successes of pilot programs in New Jersey and other states to national efforts to track and respond to the threat from heroin trafficking***.

OPPORTUNITIES

- ***Continue validation of the statewide and regional ISE concept***, and promote sharing of frameworks, tools, and initiatives in order to accelerate nationwide information sharing capabilities that work locally, regionally, and nationally against priority threats.
- Building on initial successes, ***establish procedures to federate identity, credential, and access management across agencies and private sector entities***. Use common approaches to support sharing existing capabilities across new mission areas, such as cybersecurity.
- ***Promote more mature, managed use of ISE frameworks, tools, and initiatives*** by agencies and private sector entities within their own Communities of Interest.
- ***Further align technology-related acquisition investments*** through the increased use of interoperability frameworks within *Project Interoperability*, such as the ISE Architecture Framework Grid, the ISE Standards and Specification Framework, and the ISE Common Profile.

STRENGTHEN INFORMATION SAFEGUARDING THROUGH STRUCTURAL REFORM, POLICY, AND TECHNICAL SOLUTIONS

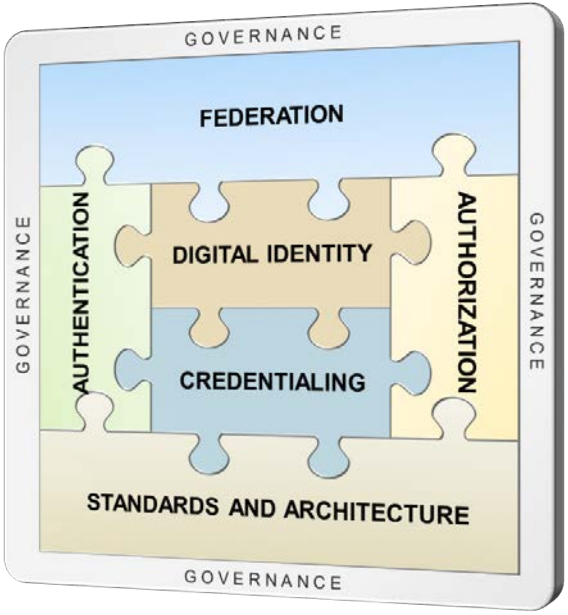
Safeguarding information and decreasing unauthorized disclosures of classified information improves success across all mission areas by improving personnel security practices, raising security awareness within the workforce, reducing risks associated with "privileged" users, and focusing greater attention on the protection of sensitive but unclassified networks.

Automated sharing of threat intelligence incidents, indicators, investigatory referrals, and victim notifications can dramatically improve cybersecurity; but the single most important thing we can do to improve cybersecurity is to improve identity, credential, and access management.

CHALLENGE

Progress toward safeguarding information has been uneven. The unauthorized disclosures of classified information in 2013 revealed vulnerabilities and shortcomings that adversely impact all ISE mission areas. Additionally, as recognized by Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and other ongoing efforts to forge legislation, cybersecurity information sharing within the Federal Government, with non-federal agencies, and with private sector entities remains a significant challenge.

Broad-based efforts to implement federated, standards-based, and interoperable identity, credential, and access management with the sensitive but unclassified and Secret fabrics continue to suffer from unaligned management practices. This figure highlights the necessary solution components, with governance binding them all together and driving effective and efficient implementation. From a strategic and policy perspective, there is complete alignment among various OMB Cross Agency Performance Goals, the National Strategy for Trusted Identities in Cyberspace, and efforts to implement the 2012 Strategy.



ACCOMPLISHMENTS

Departments, agencies, and other key ISE partners have made improvements through the following accomplishments:

- ***DHS continued development of its Enhanced Cybersecurity Services*** to share cybersecurity threat intelligence with public and private sector partners.
- ***The FBI deployed the iGuardian cyber incident reporting system***, which allows industry-based partners to report cyber intrusion incidents in real time.
- ***The Committee on National Security Systems adopted the Federal Chief Information Officer Council's Federal Identity, Credential, and Access Management framework*** for implementation on the Secret fabric. This framework is driving federal civilian agencies and is completely aligned with state and local frameworks.
- ***The Senior Information Sharing and Safeguarding Steering Committee***[8] ***determined that work has been completed on Removable Media***, one of its top priority areas.
- ***The Committee on National Security Systems will continue to monitor use of Removable Media*** to ensure ongoing compliance by departments and agencies.

OPPORTUNITIES

- The Senior Information Sharing and Safeguarding Steering Committee ***identified Continuous Diagnostics and Mitigation as an additional future priority*** for classified networks, to align with the existing priority on unclassified networks.
- ***Clarify capstone and executive agent roles and responsibilities*** as they pertain to accelerating the implementation of identity, credential, and access management.
- ***Better integrate non-federal requirements and federal requirements outside core cybersecurity agencies and programs*** by focusing on open standards and leveraging existing Information Sharing Environment and other government-wide initiatives.
- ***Strengthen the access controls for users with elevated privileges*** to classified information.
- ***Identify capability gaps***, and procure products and services as needed, to implement agencies' information security continuous monitoring strategies.
- ***Continue to develop processes and procedures to enable integrated computer network-related threat information sharing between and across agencies and private sector partners.***
- ***Extend Identity, Credential, and Access Management services to prioritized Communities of Interest***, and then expand the services on a broader scale.
- ***Continue analysis of policy and legal considerations*** that may broadly impact information sharing agreements, particularly with the Intelligence Community.

[8] Established in October 2011 by Executive Order 13587 to exercise overall responsibility and ensure senior-level accountability for the coordinated interagency development and implementation of policies and standards for the sharing and safeguarding of classified information on computer networks.

PROTECTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES

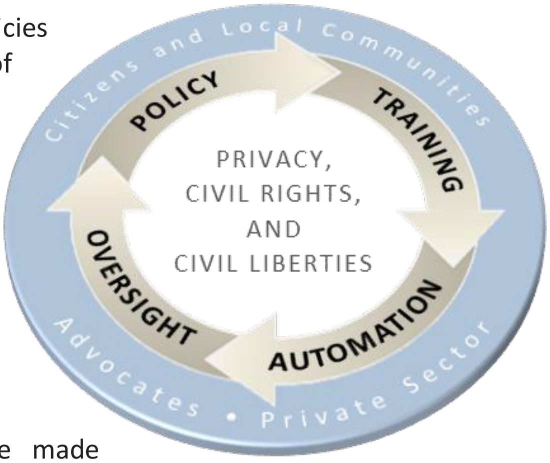
Adhering to the Rule of Law and upholding the public trust are fundamental to a legitimate ISE, and to maintaining public support for responsible information sharing. Members of the ISE must engage local communities, advocates, and the private sector to ensure that information standards and initiatives comply with applicable privacy, civil rights, and civil liberties protections, and that they are accompanied by effective oversight.

CHALLENGE

The ISE privacy, civil rights, and civil liberties (P/CR/CL) community continues to work toward the development, integration, and demonstration of P/CR/CL protections into information sharing, while reinforcing awareness and application of policies, training, and compliance through standardized compliance mechanisms.

Agencies responsible for watchlisting, threat identification, and information sharing face continuing challenges in how information is shared in accordance with P/CR/CL. These challenges include legal, policy, and technical constraints, agency practices and cultures, and public expectations.

Challenges remain in the universal adoption of P/CR/CL policies across the Federal Government. While the Department of Defense made progress this year by publishing proposed updates to its privacy and civil liberties program in the *Federal Register*, the agency has not yet finalized its privacy policy under the ISE Privacy Guidelines. All other federal agencies have adopted privacy policies as comprehensive as the President's 2005 Information Sharing Environment Privacy Guideline.


Citizens and Local Communities
POLICY
TRAINING
AUTOMATION
OVERSIGHT
PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES
Advocates • Private Sector

ACCOMPLISHMENTS

Departments, agencies, and other key ISE partners have made improvements through the following accomplishments:

- ***Establishment of an interagency effort to examine particular P/CR/CL "use cases"*** to identify the legal, policy, or technical impediments for specific watchlisting data elements that need to be shared, correlated, and retained.
- ***The adoption of written privacy policies by both federal and non-federal organizations*** has increased trust between Communities of Interest in sharing terrorism-related information, which in turn has led to more efficient and timely information exchanges in mission areas such as watchlisting and screening, and domestic law enforcement organizations.

- Within the federal ISE P/CR/CL Community of Practice, ***efforts to establish a baseline for compliance assessments indicate a slow but steady transition from ad hoc processes to a more standardized internal approach*** for P/CR/CL protections in information sharing policies and programs. For example, performance reporting from federal departments and agencies showed a 40 percent increase over last year in the development and deployment of P/CR/CL training.
- The Information Sharing and Access Interagency Policy Committee's Privacy and Civil Liberties (P/CL) Subcommittee completed and deployed ***a self-assessment worksheet for use by federal P/CR/CL officers in assessing agency-wide internal compliance*** with the implementation of ISE P/CR/CL policy and best practices.
- The National Network of Fusion Centers ***reported increased use of assessment and evaluation tools such as the P/CR/CL Compliance Verification for the Intelligence Enterprise***. Additionally, DHS and the National Network have conducted dozens of fusion center-based engagement efforts with local community-based advocacy organizations on P/CR/CL issues.
- The Privacy and Civil Liberties Oversight Board (PCLOB), established under the IRTPA, has conducted ***extensive oversight of programs related to Sections 215 and 702 of the Foreign Intelligence Surveillance Act***, and has made a series of recommendations for incorporating privacy safeguards into these programs, including provisions governing the use and dissemination of information.
- The PCLOB has also provided feedback to DHS on the draft report on implementation of Executive Order 13636 on Improving Critical Infrastructure Cybersecurity, including ***recommending the development of specific policies for sharing of personally identifiable information***.
- Created in August 2013 at the direction of the President, ***IC ON THE RECORD*** (Intelligence Community on the Record), an Office of the Director of National Intelligence blog at icontherecord.tumblr.com, ***provides immediate, ongoing, and direct access to factual information about the foreign intelligence surveillance activities of the United States Intelligence Community***.
- In April 2014, ***NCTC posted three additional documents on its public website to provide greater insight into how NCTC accesses, uses, and protects data under its stewardship***.

OPPORTUNITIES

- ***Further strengthening P/CR/CL safeguards, to include developing and supporting adoption and use of policy compliance tools across departments and agencies***, will allow for a systematic assessment of enterprise-wide implementation of P/CR/CL protection policies.
- ***Promoting more systematic, repeatable, multi-lateral, and automated information sharing agreements***, with full engagement from the P/CR/CL community, will enable standards-based approaches to privacy policy implementation, and assurance of enforcement.

MATURATION OF INITIAL INITIATIVES

The 9/11 Commission, the Markle Foundation, ISE-enabling legislation, and the *2007 National Strategy for Information Sharing* called for a "whole of government" approach to terrorism-related information sharing. The vision is to achieve a distributed, decentralized, and coordinated environment that leverages common standards and shared capabilities, delivers strengthened protections for privacy and other rights, and improves access to and discovery of information through an authorized use policy.

In the past year, local, state, and federal agencies took important steps to integrate the National Network of Fusion Centers, the Nationwide Suspicious Activity Reporting (SAR) Initiative, and interoperable sensitive but unclassified networks, achieving a critical milestone.

In particular, at the federal level, the policy, training, and engagement aspects of the Nationwide SAR Initiative are now integrated into DHS, and the technology aspects are integrated into the FBI. Additionally, we have made important progress in our efforts by reducing technology fragmentation and duplication; streamlining policy and engagement through a unified message; supporting policy-compliant discovery and access; and building on the central role of our state and local partners in governance efforts.

Through its partnership with the FBI and other agencies, DHS is leading federal efforts to support, mature, and integrate the National Network of Fusion Centers. The National Network continues to increase maturity with critical operating capabilities, serving as the key link for bi-directional threat information sharing between and across federal, state, local, tribal, and territorial agencies, and the private sector, as well as the key infrastructure for horizontal sharing between states and localities. This intelligence and information sharing extends well beyond terrorism, to the full range of priority threats in the nexus of public safety and national security. Increasingly the National Network is engaging in trusted and secure collaboration with other field-based intelligence and information sharing entities including, but not limited to, the Regional Information Sharing System, High Intensity Drug Trafficking Areas, and the Joint Terrorism Task Forces. The DOJ and the Office of the Director of National Intelligence, among other federal partners, have made and continue to make sustained contributions.

It is noteworthy that the National Network, via the National Fusion Center Association, has developed a three year strategy in response to the recommendations in the July 2013 House of Representatives Homeland Security Committee Majority Staff Report on the National Network of Fusion Centers.[9] This integrated effort includes all of the major law enforcement associations and state and local field-based entities, and holds the promise of bringing the policy and governance process between U.S. levels of government to a new level of maturity.

In keeping with the original whole-of-government vision for the ISE, the National Network has become a core national security and public safety asset, with each center owned by its sponsoring state or local agency. While there are continued opportunities to improve performance and

[9] *2014–2017 National Strategy for the National Network of Fusions Centers*, July 2014.

integration and reduce fragmentation, these events mark an important milestone in the delivery of the ISE.

WAY FORWARD

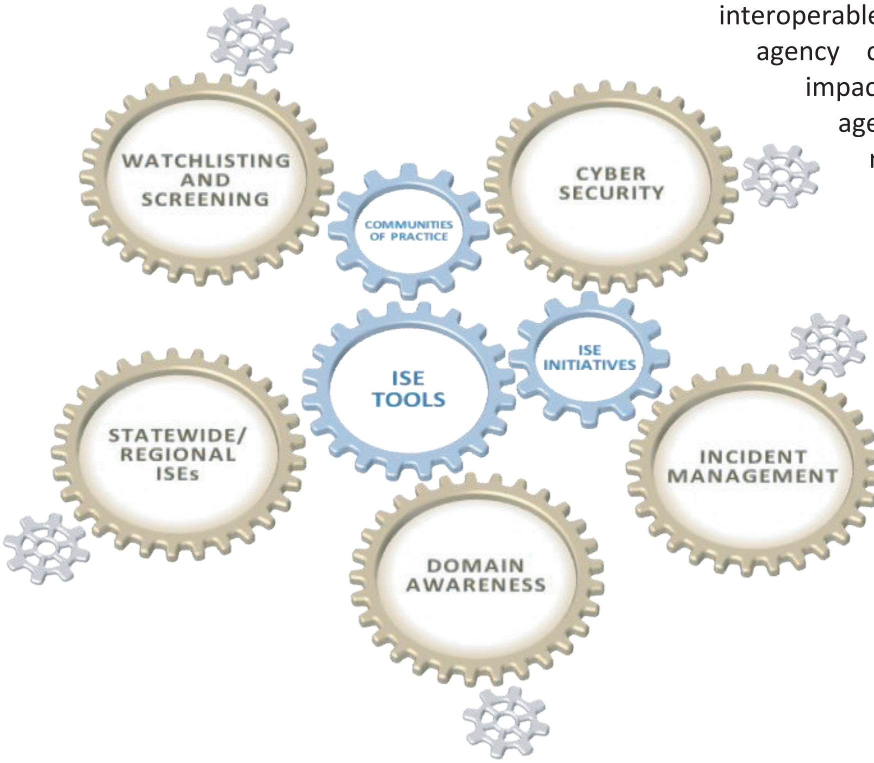
The challenges and accomplishments highlighted in this report demonstrate the continued value added to our nation's security of the vision for a decentralized, distributed, and coordinated Information Sharing Environment.

To deliver national security through responsible information sharing, we must support agency efforts to improve governance, and work with the White House to support interagency efforts. Critical support must come through aligning agency management practices—internally and externally—to strengthen the linkages between planning, resourcing, and established accountability.

Over the next year we will continue to bridge Communities of Interest with Communities of Practice to support mission partners in delivering capabilities against the targeted mission outcomes. Coordinated via the Information Sharing and Access Interagency Policy Committee, agencies must continue to implement the 2012 Strategy by identifying and prioritizing participation in Communities of Interest, based on shared mission equities against common priority threats.

We will start with the five highlighted mission-focused Communities of Interest, and organize around transnational organized crime. Within all of these Communities of Interest, we expect discrete, coordinated, and focused efforts, leading to the delivery of interoperable, reused, and in some cases shared agency capabilities to accelerate mission impact. Constraints on progress include an agency's capacity to transform, its maturity and alignment of management practices, and its budget limitations.

Communities of Interest will be able to use this continuous cycle to accelerate progress on their responsible information sharing challenges, using ISE tools and initiatives, accessed via Communities of Practice.



ing
ation
Technology
standards
policies
protections
interoperability
processes
privacy
unclassified
governance
enable
strategic
areas
continue
Federal
Protection
new
infrastructure
guidance
personnel
fusion
security
mission
Maritime
officers
effort
Office
law
Department
local
data
U.S.
terrorism
also
community
across
Agency
government
state
technical
provides
products
systems
NIEM
Performance
Services
best
levels
capability
Criminal
development
analysis
activities
work
analysts
key

Program Manager, Information Sharing Environment
Washington, D.C. 20511

202.331.2490

www.ise.gov

- @shareandprotect
- fb.me/informationsharingenvironment
- http://lnkd.in/zaCB97
- youtube.com/shareandprotect
- ise.gov/blog
- ise.gov/email